

NAVAL WAR COLLEGE
Newport, R.I.

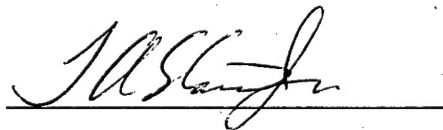
SOME PRINCIPLES OF NETWORK-CENTRIC WARFARE: A Look at How
Network-Centric Warfare Applies to the Principles of War

By

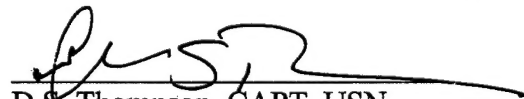
Thomas A. Slais, Jr.
Lieutenant Commander, U.S. Navy

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.



05 February 1999



D.S. Thompson, CAPT, USN
Faculty Advisor

DISTRIBUTION STATEMENT A
Approved for Public Release
Distribution Unlimited

BTIC QUALITY INSPECTED 4

19990520 055

1. Report Security Classification: UNCLASSIFIED			
2. Security Classification Authority:			
3. Declassification/Downgrading Schedule:			
4. Distribution/Availability of Report: DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.			
5. Name of Performing Organization: JOINT MILITARY OPERATIONS DEPARTMENT			
6. Office Symbol: NWC Code 1C		7. Address: NAVAL WAR COLLEGE 686 CUSHING ROAD NEWPORT, RI 02841-1207	
8. Title (Include Security Classification): SOME PRINCIPLES OF NETWORK-CENTRIC WARFARE: A Look at How Network-Centric Warfare Applies to the Principles of War (u)			
9. Personal Authors: Thomas A. Slais, Jr., Lieutenant Commander, U.S. Navy			
10. Type of Report: FINAL		11. Date of Report: 05 February 1999	
12. Page Count: 26 (including cover)			
13. Supplementary Notation: A paper submitted to the Faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.			
14. Ten key words that relate to your paper: Network-Centric Warfare, Principles of War, Operational Art, Information Superiority			
15. Abstract: The principles of war are one of the most important and enduring facets of operational art. Network-centric warfare, enabled by technology of the information age, is a new concept the U.S. is adopting in order to fight faster, cheaper and better in the twenty-first century. This analysis shows that network-centric warfare applies to the principles of war—specifically, the principles of mass, offensive, unity of command and security. With regard to mass, the information, sensor and engagement grids of network-centric warfare, will enable dispersed forces to mass effects by coordinating location, identification and targeting information from sensors to rapidly employ long range, precision fires, using shared information from a common operational picture. With respect to offensive, network-centric warfare will effectively allow us to dominate factor time and operate inside the enemy's decision cycle. Thus, it will enhance our ability to seize and retain the initiative and preserve our freedom of action. As it applies to unity of command, network-centric warfare will aid tactical commanders, armed with a clearly defined commander's intent from the operational level, to maintain the situational awareness required to self-synchronize and act on opportunities while maintaining unity of effort toward achieving the operational commander's objective. Finally, with regard to security, network-centric warfare will increase our ability to achieve battle space dominance through information superiority. However, we will be increasingly dependent on protecting our C4I systems to ensure that we can achieve our military objectives. The tie that binds network-centric warfare to the principles of war is that it will enable enhanced situational awareness, which will improve our ability to abide by the principles in a more sufficient manner.			
16. Distribution / Availability of Abstract:	Unclassified X	Same As Report X	DTIC Users
17. Abstract Security Classification: UNCLASSIFIED			
18. Name of Responsible Individual: CHAIRMAN, JOINT MILITARY OPERATIONS DEPARTMENT			
19. Telephone: 841-6461		20. Office Symbol: 1C	

Abstract

The principles of war are one of the most important and enduring facets of operational art. Network-centric warfare, enabled by technology of the information age, is a new concept the U.S. is adopting in order to fight faster, cheaper and better in the twenty-first century. This analysis shows that network-centric warfare applies to the principles of war—specifically, the principles of mass, offensive, unity of command and security. With regard to mass, the information, sensor and engagement grids of network-centric warfare, will enable dispersed forces to mass effects by coordinating location, identification and targeting information from sensors to rapidly employ long range, precision fires, using shared information from a common operational picture. With respect to offensive, network-centric warfare will effectively allow us to dominate factor time and operate inside the enemy's decision cycle. Thus, it will enhance our ability to seize and retain the initiative and preserve our freedom of action. As it applies to unity of command, network-centric warfare will aid tactical commanders, armed with a clearly defined commander's intent from the operational level, to maintain the situational awareness required to self-synchronize and act on opportunities while maintaining unity of effort toward achieving the operational commander's objective. Finally, with regard to security, network-centric warfare will increase our ability to achieve battle space dominance through information superiority. However, we will be increasingly dependent on protecting our C4I systems to ensure that we can achieve our military objectives. The tie that binds network-centric warfare to the principles of war is that it will enable enhanced situational awareness, which will improve our ability to abide by the principles in a more sufficient manner.

Preface

This paper addresses how network-centric warfare applies to the principles of war. Since 1949 the principles of war for the U.S. military have remained as follows: mass, objective, offensive, security, economy of force, maneuver, unity of command, surprise and simplicity. The premise of this paper is that network-centric warfare neither eliminates nor alters the principles of war. Instead it essentially enables the achievement of many of the principles of war in a more sufficient manner. The scope of this analysis will look at how network-centric warfare applies to the principles of mass, offensive, unity of command and security. Although network-centric warfare applies to all the principles, those addressed herein were largely chosen due to their perceived potential to be affected by the technological advances and the force structure challenges the U.S. military is dealing with today and will continue to face in the future.

More specifically, the principle of mass was chosen because in a time of force reductions and constantly growing military commitments, how will the U.S. military be able to mass effects in the future to fight faster, cheaper and better? Is network-centric warfare the answer? The principle of offensive was chosen for its emphasis on seizing the initiative to decisively achieve our military objectives. Will the technological advances brought forth by network-centric warfare enable a speed of decision capability superior to our enemy and provide us a decisive advantage? The principle of unity of command was chosen because many military professionals assert that the enhanced situational awareness at all levels provided by network-centric warfare could serve to detract from this principle. Their argument is that it will enable tactical commanders to act with too much initiative, or it will enable operational commanders to micromanage

the tactical situation. Is this in fact the case? Finally, the principle of security was chosen because force protection and our ability to maintain freedom of action are critical to ensuring mission accomplishment. If network-centric warfare provides battle space dominance, force protection should follow suit. But if network-centric warfare presents critical weaknesses in our C4I structure, that can potentially become critical vulnerabilities at the hands of a capable enemy, then the need to highlight this application is equally important.

The purpose of this paper is to show that network-centric warfare applies to the principles of war. In doing so, it will analyze and provide argument to answer these questions. It will also show that network-centric warfare is not a threat to operational art, but rather a tool to enhance human decision making and enable us to more sufficiently abide by the guidance set forth by the principles of war.

Introduction

“The principles of war guide war fighting at the strategic, operational, and tactical levels. They are the enduring bedrock of US military doctrine.”¹

The principles of war are one of the most important facets of operational art--so important in fact military establishments of several countries around the world have principles by which they conduct war. The Army first defined the principles of war for the U.S. military in 1921. They were renamed in 1939 but virtually held their original definitions and meanings. After being heavily tried and tested in the European and Pacific theaters during World War II, they were again renamed in 1949, but like previous revisions, were largely unchanged. Over the years, the principles of war have endured several revolutions in military affairs and much professional scrutiny; but they remain today as they did in 1949. Regardless of changes in the nature of war throughout the twentieth century, the principles of war have endured the test of time.

As we approach the dawn of the twenty-first century, we have passed from the industrial age into the information age and, as a result, the nature of war is again being redefined. According to Admiral Jay Johnson, Chief of Naval Operations, we are experiencing “...a fundamental shift from what we call platform-centric warfare to something we call network-centric warfare...”² Network-centric warfare is warfare that is comprised of a network of participating sensors, platforms and forces, cooperatively acting on fused information from a common operating picture, in order to achieve a military objective. The synergy created by the combination of enhanced situational awareness and force synchronization is the dominant factor. In contrast, platform-centric warfare is the traditional, attrition based form of warfare of the industrial age where forces (at least naval forces) were built around a major platform, using their own sensors and weapons to engage a

target to accomplish a military objective. Network-centric warfare promises enhanced situational awareness, increased speed of command, massed firepower from dispersed forces and self-synchronized command and control--command and control from the bottom up instead of from the traditional, top down approach.³ This approach is heavily dependent on moving information throughout a network of grids--more specifically, "...an operational architecture with three critical elements: sensor grids and transaction (or engagement) grids hosted by a high-quality information backplane [provided by information grids]."⁴ Maintaining the advantage with network-centric warfare will be highly dependent on achieving and maintaining information superiority.

Network-centric warfare, enabled by technology of the information age, is a new concept that U.S. forces are adopting in order to fight faster, cheaper and better in a time when tight military budgets and force reductions are military realities. Given these realities, growing American world commitments demand efficiencies that network-centric warfare can provide. But does network-centric warfare apply to the principles of war, which up until now have endured the test of time? Network-centric warfare does apply to the principles of war; however, the degree of application varies with each principle. The following analysis will highlight the application of network-centric warfare to selected principles of war by looking at the principles of mass, offensive, unity of command and security. It will also highlight the premise that the enhanced situational awareness, network-centric warfare provides the war fighter, is the tie that binds it to the principles of war.

Network-Centric Warfare Applied to the Principle of Mass

“The purpose of mass is to concentrate the effects of combat power at the place and time to achieve decisive results.”⁵

A look at the Napoleonic wars shows that this principle referred to a massing of *forces* in time and place, against a decisive military objective, and contributed greatly to motivating *levee en masse*—an early nineteenth century version of mass conscription. Using the principle of mass, Napoleon fielded huge armies numbering in the hundreds of thousands to defeat his adversaries and conquer the European continent. In the industrial age, massed forces were thought to be of equal importance. The battleship building agreements among the United States, Britain and Japan during the period between the first and second world wars underscored the fact that numbers and size of capital ships signified naval power. This basic concept was carried forward into the 1980's when U.S. Navy Secretary John Lehman launched his initiative to build the 600-ship navy in order to provide credible deterrence against the Soviet Union. Massing forces to achieve military objectives has traditionally been associated with platform-centric warfare--where the aircraft carrier and its air wing, augmented by surface and subsurface Tomahawk shooters, is the center of battle group striking power. Even today, when staffs conduct deliberate and crisis action planning for medium to high intensity ground operations, relative combat strength is measured by numbers of armored division equivalents (ADE's) between adversaries. Massing forces is still important. However, over the last few years, the U.S. military's emphasis has shifted from massing forces to massing *effects*.

Network-centric warfare applies to the principle of mass in that it will enhance our capability to mass effects. Using the information, sensor and engagement grids of the network, dispersed forces will mass effects by coordinating location, identification and

targeting information from sensors to rapidly employ long range, precision fires, using shared information from a common operational picture. Also, by linking combat logistic support on the information grid, the resulting ammunition expenditure will be immediately entered as data to facilitate re-supply and force readiness monitoring by the operational commander. These attributes of network-centric warfare not only highlight its application to the principle of mass, but also show its direct relation to the operational concepts of dominant maneuver, precision engagement, full-dimensional protection and focused logistics in Joint Vision 2010.⁶

Parallels may be drawn between network-centric warfare and concepts of current Air Force cooperative targeting of enemy surface to air missile systems between F-16CJ (Suppression of Enemy Air Defense's (SEAD) as its primary mission) and RC-135 Rivet Joint aircraft. During these cooperative operations, information is shared among aircraft by using the Improved Data Modem (IDM) to digitally data-link shared targeting data. This action is analogous to moving data along the *information* grid. The system is most often implemented by using the RC-135 to pass enemy surface-to-air missile (SAM) identification and location data to participating F-16CJ aircraft, which also use their own HARM Targeting System (HTS) pods as sensors. This is analogous to coordinating sensors on the *sensor* grid. This information is then incorporated into the F-16CJ's Harm Targeting System to employ High-speed Anti-Radiation Missiles (HARM) against targets designated by the RC-135, or against targets shared among the division of four F-16CJ aircraft. This is analogous to target designation using an *engagement* grid. Targeting data to the RC-135 is either derived from its own on-board sensors or received from space-based sensors.

Vice Admiral Arthur Cebrowski and Dr. John Garstka put forth an example of how network-centric warfare will have a profound impact on the future effectiveness of joint SEAD. They assert that "...through co-evolution of systems, organization, and doctrine, we introduce other shooters that are capable of attacking SAM sites, such as ATACMS [Army Tactical Missile System], and employ them as part of an engagement grid."⁷ Instead of relying mostly on HARM and electronic jamming as primary SEAD weapons, network-centric warfare will enable the U.S. military to conduct joint SEAD using networked hard-kill weapon systems with much greater accuracy, lethality and overall effectiveness. Through enhanced battle space awareness and cooperative target engagement, the previously discussed examples show how network-centric warfare can be used to mass effects to neutralize enemy air defenses.

An example of how network-centric warfare will mass effects to support Operational Maneuver From The Sea (OMFTS) is the 'Ring of Fire' concept used to employ Naval Surface Fire Support (NSFS). 'Ring of Fire' can be employed by ships from dispersed locations from ranges of up to 1000 miles. It would not only effectively support troops on the ground but would also deliver a shocking effect to the enemy by massing precision firepower from dispersed long range locations into a concentrated space at a given time.

"Each ship in the ring will have the ability to launch land-attack weapons from other ships in the ring remotely...In effect, the Ring of Fire is a battle group local area network comprising a joint fire control network and a joint planning network. The ring provides a distributed collaborative method to plan scheduled fires for interdiction and long-range strike."⁸

Fire support may be apportioned and executed preemptively at the operational commander level, or may be requested digitally by troops on the ground who would also provide

targeting data to the shooters. As in previously discussed examples of network-centric warfare, ordnance expenditure is tracked for automated situational awareness and re-supply.

However, F. J. "Bing" West expressed concerns about the viability of 'Ring of Fire' in a recent article published in U.S. Naval Institute's *Proceedings*. He argues that this network-centric concept of providing massed effects in support of OMFTS will be limited due to a shortage of firepower available to support the engagement grid.⁹ 'Ring of Fire' was developed with the premise that arsenal ships would be available to support the high demand for surface fired ordnance. With recent cancellation of the arsenal ship program, ammunition logistics and apportionment may become a more critical factor. However, the effects that are massed by network-centric warfare include more than just delivering massive quantities of hard-kill ordnance. The increase in situational awareness and resource management capabilities it provides will serve to mitigate potential ammunition shortfalls. By gaining effectiveness through coordination and enhanced weapons accuracy, the benefits of adopting network-centric warfare as a key element in massing effects against the enemy far outweigh the risks of ignoring it as a tool to enable the operational commander to achieve his overall objectives.

The previous examples clearly illustrate the direct application network-centric warfare will have in achieving the principle of mass. They emphasize that dispersed forces networked into a common information, sensor and engagement grid can dominate the battle space by maintaining information superiority and situational awareness in order to mass effects of combat power at a decisive place and time against the enemy.

Network-Centric Warfare Applied to the Principle of Offensive

“The purpose of an offensive action is to seize, retain, and exploit the initiative...while maintaining freedom of action and achieving decisive results.”¹⁰

The key element in this definition of the principle of offensive is seizing the initiative.

This applies whether a force is on the offensive, or on the defensive looking for an opportunity to shift to the offensive. Network-centric warfare supports this principle primarily through information superiority.

At first glance, it may seem like the problem of seizing the initiative through network-centric warfare is oversimplified. In order to achieve information superiority and bring weapons to bear against the enemy, targets must first be detected, classified, located and properly identified. In situations like Bosnia or Somalia, where targets were either concealed or blended into the local populace, target identification and location becomes a difficult problem. But, multiple networked sensors of various types increase the probability of reliable acquisition. Against a threat from a third world agrarian society, conducting asymmetrical warfare against U.S. forces, the best sensor to sort out hostile from non-hostile may be the ‘grunt on the ground’. This information must also be fed into the net.

As information is correlated and fused (synthesized) from the myriad of synchronized sensors on the sensor grid, it will enhance information accuracy. The resulting information from synthesized sensor data will help build situational awareness, by providing a common operational picture on the information grid. It then becomes actionable or “decision ready” information. Based on this information, the engagement grid rapidly pairs targets to shooters in geographically dispersed areas. “[Using] high speed algorithms [the engagement grid] can rapidly determine near optimal weapon-target pairings subject to time varying constraints, such as number and value of remaining targets, the number of remaining shooter

rounds, and the probability of kill of remaining rounds.”¹¹ This explanation of information, sensor and engagement grid interaction demonstrates how network-centric warfare will enable friendly forces to self-synchronize their actions and achieve speed of command--to make decisions and act faster and more intelligently than the enemy. Network-centric warfare effectively allows friendly forces to dominate factor time and operate inside the enemy's Observe, Orient, Decide and Act (OODA) loop.¹² In doing so, the enemy is denied the time to observe the battle situation and orient his forces. He is therefore denied the ability to make decisions or is forced to make hasty ones which severely denies his ability to act effectively. As this occurs, the situation develops an accelerating rate of change on the battlefield with which the enemy can neither cope nor counter--enemy courses of action are effectively 'locked out' and friendly courses of action are 'locked in'.¹³ These examples support the premise that network-centric warfare applies to and supports the principle of offensive. The conditions brought about by network-centric warfare will serve to have an 'anti-massing' effect on the enemy's capability by denying him the same ability to seize the initiative and force our courses of action. At the same time, it will enhance our ability to seize and retain the initiative and preserve our freedom of action. The end result will be first battle space superiority, then battle space dominance which eventually will lead to the enemy's psychological or physical defeat.

Network-Centric Warfare Applied to the Principle of Unity of Command

“The purpose of unity of command is to ensure unity of effort under one responsible commander for every objective.”¹⁴

The American way of war is to plan and execute military operations using centralized command and decentralized execution. To ensure unity of effort, operational commanders focus on issuing their subordinates a clearly defined mission objective, a concept of

operations and, above all, a clearly articulated commander's intent. The simple explanation for this procedure is to help guide the actions of subordinate commanders and enable them the flexibility to shift effort as required by changing situations in battle. When the fog of war and friction of battle degrade situational awareness and chaos erupts, the overall objective and the commander's vision of the desired end state will remain clear to the tactical commanders and their forces. Network-centric warfare applies to maintaining unity of command/effort and will not degrade this principle. Synthesized information moved throughout the information grid will provide a common operational picture to the entire force. Network-centric warfare will aid tactical commanders, armed with a clearly defined commander's intent, to coordinate their forces and maintain the situational awareness required to either take action on opportunities that may pre-empt enemy action, or react with such speed and agility as to negate the enemy's initiative. This is the meaning of self-synchronization and speed of command.

Some argue that the enhanced situational awareness network-centric warfare brings will provide subordinate commanders with enough knowledge to act with too much initiative. Others assert that enhanced situational awareness at all levels will entice the operational commander into micromanaging the tactical situation. But if the operational commander's intent is clearly understood at the tactical level and enhanced situational awareness produces opportunities, that if exploited would defeat the enemy faster, then it is the duty of the tactical commander to act on those opportunities. Moreover, instead of micromanaging, most good commanders would still trust the judgement of their commanders to act on their guidance, just as they do today. If anything, enhanced situational awareness will enable the operational commander to plan his or her next move based on known facts

instead of having to rely on commander's intuition or *coup d'oeil*.¹⁵ Network-centric warfare will enable the operational commander to project his next course(s) of action further into the future, rather than entice him into becoming more directly involved at the tactical level.

Command and control characteristics of network-centric warfare may be compared to those of 'cyberwar'—a term developed by Dr. John Arquilla and Dr. David Ronfeldt in a Rand National Defense Research Institute study on the evolution of warfare as a result of the information revolution. They propose the following on networked C2 structures.

"Moving to networked structures may require some decentralization of command and control, which may be resisted in light of...[the premise] that the new technology would provide greater central control of military operations. But decentralization is only part of the picture; the new technology may also provide greater "topsight"—a central understanding of the big picture that enhances the management of complexity."¹⁶

Network-centric warfare will provide the operational commander and his subordinate commanders the flexibility to decentralize and execute more quickly and handle more complex situations than in a non-networked environment. But it will still provide the operational commander better 'topsight' to adjust his focus of effort using methods such as video teleconferencing (VTC) if needed.¹⁷ Command structure may have to change in order to capitalize on speed of command from decentralization. To do this, it may be necessary to eliminate a command echelon between the operational and tactical levels, thus creating a flatter organization. However, further discussion regarding restructured levels of command and control requires a level of detail beyond the scope of this paper.

Networked command and control nodes could enable linked participation by other government agencies, non-government organizations and private volunteer organizations while planning and conducting military operations. In these situations, a clearly defined objective, commander's intent, desired end state and the ability to garner civil cooperation

are particularly critical to ensure unity of effort because unity of command may not be possible. For example, the information grid could provide the means for interagency interaction to assist in maintaining more efficient host nation support to logistics. Here, elements of network-centric warfare would prove invaluable to enable unity of effort.

In a recent article, Prof. Thomas P. M. Barnett expressed concern about allied and coalition participation in U.S. military operations in a network-centric environment. He cautions that "[t]hese states barely can afford the shrinking force structures they now possess, and if network-centric warfare demands...tremendous preconflict [sic] investments in data processing...then the future of coalition warfare looks bleak indeed."¹⁸ The U.S. military recognizes the seriousness of this challenge. A major focus of the Joint Warrior Interoperability Demonstrations (JWID) for 1997 and 1998 was C4I interoperability among allies. In both demonstrations, Australia, Canada, New Zealand, the United Kingdom and the United States were the representative allied group. "JWID 98 expanded on the utility of the coalition secret-high CWAN [coalition wide area network] to be used as a Network Centric Warfare tool, including the feasibility of setup of a CWAN in support of forward deployed contingencies and network management."¹⁹ The use of commercial off-the-shelf computer systems (COTS) and internet technologies such as Transmission Control Protocol/Internet Protocol (TCP/IP), Hyper Text Markup Language (HTML), web browsers, search engines and Java TM computing architecture will enable allied systems to interact with U.S. systems.²⁰ Thus, it will allow network-centric computing to support coalition warfare. This works well with our long standing allies, with whom we regularly share technology, equipment and training experience in combined exercises. But, how do we integrate future *ad hoc* coalition partners into a network-centric war, whose countries have not yet fully entered the

information age? If the United States is unable or unwilling to train and equip underdeveloped coalition partners with the tools of network-centric warfare, those partners may have to be assigned low risk duties where they will not pose a liability to the overall effort or be "integrated" off line. With the exception of the last problem, the previous analysis clearly supports the premise that network-centric warfare not only applies to but also enhances the principle of unity of command.

Network-Centric Warfare Applied to the Principle of Security

"The purpose of security is to never permit the enemy to acquire unexpected advantage. Security enhances freedom of action by reducing friendly vulnerability to hostile acts, influence or surprise."²¹

Network-centric warfare's application to the principle of security cuts both ways like a double-edged sword. On one hand, it provides dominant battle space awareness and the synergistic effect of dispersed forces cooperatively protecting each node of the sensor and engagement grids, which is a revolutionary advancement in force protection. On the other hand, the success of network-centric warfare and the survival of those who use it depend on protecting the information, sensor and engagement grids and the associated C4I systems from either an organized information warfare offensive or a 'terrorist' attack from a rogue hacker. In either case, the importance of security in network-centric warfare is critical.

Preliminary examples of how network-centric warfare will aid in force protection exist today. Cooperative Engagement Capability (CEC) is designed to enhance force defense by fusing sensor data from various platforms--air and surface--to develop a composite target track with greater speed and accuracy than is possible from a single platform's sensor. CEC can then pass the designated track to any surface shooter that is able to engage the target.

“Even if its own sensors have not yet acquired...[an inbound missile], a ship can use the composite track to engage an attacking anti-ship missile within its weapons range.”²²

The following example highlights the potential effectiveness of CEC as a network-centric force defense tool.

“In a 1996 demonstration in Hawaii, a CEC-equipped Aegis cruiser--using composite track data provided by...[an off board] CEC-equipped radar and tracker/illuminator...launched four Standard surface-to-air missiles (SAMs) that destroyed, at ranges more than three times greater than previously achievable, four sea-skimming drone targets that were well beyond the ship’s radar horizon.”²³

This networked engagement capability would be particularly useful in protecting the force in the littorals from a pop-up anti-ship missile attack, and is just one example of how network-centric warfare could enhance our ability to abide by the principle of security more sufficiently. The CEC concept may also be a network-centric application that could aid Theater Ballistic Missile Defense in the future.

Network-centric warfare’s system of grids may be analyzed as one of our critical weaknesses because of its complexity and our future dependence on it to fight effectively. Against a capable adversary, it may also be one of our critical vulnerabilities. Most military professionals realize the power of information warfare. In fact network-centric warfare could be used as a tool to conduct offensive information warfare against a hostile nation. Joint Doctrine for Command and Control Warfare (C2W) defines information warfare as follows:

“...[A]ctions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while defending one’s own...”²⁴

But Clausewitzian theory of the reciprocal nature of war, reminds us that any adversary with the capability to conduct information warfare is likely to use it against the United States, particularly if the United States is conducting offensive information warfare operations

against them.²⁵ The bottom line is, if we are going to depend on a "system of systems" for our national security, we must protect it. But this may be easier said than done.

Because of their stovepipe nature, legacy C4I systems are relatively secure from intrusion. However, COTS computing systems and software, the same systems that will make network-centric warfare feasibly affordable for not only the United States but also our allies, are extremely vulnerable because of their commonality with the commercial sector. Also, with an increase in U.S. military involvement in operations other than war, there is a potential for more non-government organizations to participate in the net. This may serve to exacerbate our C4I vulnerability.

The U.S. Navy takes a multi-layered approach to systems security called 'defense in depth.'

"Defense in depth...is a risk management approach to security that accepts the chance that an attacker may get through one or two layers of defense, but the probability of the attacker getting through all layers is acceptably low. Driving this probability down can be accomplished only if each layer performs both intrusion detection and firewall functions."²⁶

Risk management may not be enough to protect what may be one of our future critical vulnerabilities. Total network-centric security may need to be further enhanced through the use of defensive information warfare. Current proposals exist to implement deception logic into our systems, which would not only detect an unauthorized intrusion but would also present the intruder with believable but bogus information to exploit and manipulate.²⁷

Network-centric warfare will increase our ability to achieve battle space dominance through information superiority. However, we will be increasingly dependent on protecting our C4I systems to ensure that we can achieve our military objectives. Network-centric warfare's

application to the principle of security is clear. Based on this analysis, it would be prudent for the commander to always be mindful of this principle when employing it.

Situational Awareness: The Tie That Binds Network-Centric Warfare to the Principles of War

“One reason we say that no plan survives initial contact with the enemy is because situational awareness does not. In platform-centric military operations, situational awareness steadily deteriorates. Network-centric operations...create a higher awareness and allow it to be maintained.”²⁸

In analyzing the applicability of network-centric warfare to the principles of mass, offensive, unity of command and security, a reoccurring element that contributes to each application is situational awareness. Enhanced situational awareness for the commander and his forces is the dominant factor that is behind the power of network-centric warfare. Similar to the principles previously discussed, it too contributes to achieving the overall objective, which is arguably the most important of all the principles of war. Many assert that the success of network-centric warfare is based on its ability to provide information superiority. While this is one of its attributes, it is only a part of what is required to successfully conduct military operations. Lt Gen Paul K. Van Riper, USMC, had the following to say in his last address to Congress on the subject of information superiority. “Without a doubt, information is important, but all the information in the world is useless unless it contributes to effective decision making in battle.”²⁹ Clearly, information is not enough. It is knowledge that counts. Knowledge is the human assimilation of fused information to gain situational awareness of the battle space. Knowledge of the situation is not only important in planning an operation; it is also critical in real time execution specifically to maintain flexibility, speed and agility. Situational awareness is a by-product of the synergistic reaction that occurs when combining the sensor, information and engagement grids with the human element. It is a key factor in

linking network-centric warfare to the other principles of war and is absolutely essential in seizing and maintaining the advantage in battle.

Conclusion

The principles of war are one of the most important facets of operational art. The lessons they provide are timeless and have been written in blood. Network-centric warfare, enabled by technology of the information age, is a new concept that U.S. forces are adopting in order to fight faster, cheaper and better in the twenty-first century. This analysis has shown that network-centric warfare applies to the principles of war—specifically, the principles of mass, offensive, unity of command and security.

With regard to mass, the information, sensor and engagement grids of network-centric warfare, will enable dispersed forces to mass effects by coordinating location, identification and targeting information from sensors to rapidly employ long range, precision fires, using shared information from a common operational picture. With respect to offensive, network-centric warfare will effectively allow us to dominate factor time and operate inside the enemy's decision cycle. Thus, it will enhance our ability to seize and retain the initiative and preserve our freedom of action. As it applies to unity of command, network-centric warfare will aid tactical commanders, armed with a clearly defined commander's intent from the operational level, to maintain the situational awareness required to self-synchronize and act on opportunities while maintaining unity of effort toward achieving the operational commander's objective. Finally, with regard to security, network-centric warfare will increase our ability to achieve battle space dominance through information superiority. However, we will be increasingly dependent on protecting our C4I systems to ensure that we can achieve our military objectives. Network-centric warfare's

application to the principles of war is reinforced by the fact that it will enable enhanced situational awareness, which will improve our ability to abide by the principles in a more sufficient manner.

Network-centric warfare will never replace the human element in war, nor is it meant to. But it will enhance the human capability to make informed decisions faster, and employ our forces with such efficiency and lethality as never before. Many military professionals are skeptical about the future of war fighting in a network-centric warfare environment. Perhaps the proven application of such a revolutionary concept as network-centric warfare, to such a timeless facet of operational art as the principles of war, is the first step in relieving their skepticism.

Notes

¹ U.S. Joint Chiefs of Staff, Doctrine for Joint Operations (Joint Pub 3-0) (Washington D.C.: February 1, 1995), A-1.

² Admiral Jay Johnson, quoted in Vice Admiral Arthur K. Cebrowski, U.S. Navy and John J. Garstka, "Network-Centric Warfare, Its Origin and Future." U.S. Naval Institute Proceedings, January 1998, 29.

³ Vice Admiral Arthur K. Cebrowski, U.S. Navy and John J. Garstka, "Network-Centric Warfare, Its Origin and Future." U.S. Naval Institute Proceedings, January 1998, 32, 33.

⁴ *Ibid*, 32.

⁵ U.S. Joint Chiefs of Staff, Doctrine for Joint Operations (Joint Pub 3-0) (Washington D.C.: February 1, 1995), A-1.

⁶ U.S. Joint Chiefs of Staff, Joint Vision 2010 (Washington D.C.: GPO, 1996), 19.

⁷ Vice Admiral Arthur K. Cebrowski, U.S. Navy and John J. Garstka, "Network-Centric Warfare, Its Origin and Future." U.S. Naval Institute Proceedings, January 1998, 32.

⁸ Lieutenant Commander Ross Mitchell, U.S. Navy, "Naval Fire Support, Ring of Fire." U.S. Naval Institute Proceedings, November 1997, 55.

⁹ F.J. West, Jr., "Ring of Fire or Ring of Smoke?" U.S. Naval Institute Proceedings, November 1998, 39.

¹⁰ U.S. Joint Chiefs of Staff, Doctrine for Joint Operations (Joint Pub 3-0) (Washington D.C.: 1 February 1995), A-1.

¹¹ U.S. Joint Chiefs of Staff, "Observations on the Emergence of Network-Centric Warfare." Network-Centric Warfare Information Paper. 16 December 1997.
<<http://www.dtic.mil/jcs/j6/education/warfare.html>> (6 January 1999).

¹² The Observe Orient Decide Act loop was originally coined and developed by the late Colonel John Boyd, USAF (Ret).

¹³ Vice Admiral Arthur K. Cebrowski, U.S. Navy and John J. Garstka, "Network-Centric Warfare, Its Origin and Future." U.S. Naval Institute Proceedings, January 1998, 33.

¹⁴ U.S. Joint Chiefs of Staff, Doctrine for Joint Operations (Joint Pub 3-0) (Washington D.C.: February 1, 1995), A-2.

¹⁵ *Coup d'oeil* is a French term used by Carl Von Clausewitz to refer to the inward eye--the intuition and creative genius of a commander. See Carl Von Clausewitz, On War, Michael Howard and Peter Paret ed. (Princeton: Princeton University Press, 1984), 102.

¹⁶ John Arquilla and David Ronfeldt, Cyberwar is Coming. (Santa Monica: Rand National Defense Research Institute, 1992), 6-7.

¹⁷ VTC enhances situational awareness among commanders and helps to ensure coordinated effort is focused on the objective because verbal and nonverbal communication cues are transmitted and received.

¹⁸ Thomas P.M. Barnett, "The Seven Deadly Sins of Network-Centric Warfare." U.S. Naval Institute Proceedings, January 1999, 36.

¹⁹ U.S Atlantic Command, JWID98 Post Demonstration Report (Norfolk, VA: 1998) Executive Summary.

²⁰ Vice Admiral Arthur K. Cebrowski, U.S. Navy and John J. Garstka, "Network-Centric Warfare, Its Origin and Future." U.S. Naval Institute Proceedings, January 1998, 30.

²¹ U.S. Joint Chiefs of Staff, Doctrine for Joint Operations (Joint Pub 3-0) (Washington D.C.: February 1, 1995), A-2.

²² Leslie West, "Exploiting the Information Revolution, Network-Centric Warfare Realizes Its Promise." Sea Power, March 1998, 40.

²³ Ibid.

²⁴ U.S Joint Chiefs of Staff, Joint Doctrine for Command and Control Warfare (C2W) (Joint Pub 3-13.1) (Washington D.C.: February 7, 1996), I-3.

²⁵ Michael I. Handel, Masters of War. 2nd revised and expanded ed. (Portland, OR: Frank Cass, 1996), 79.

²⁶ Vice Admiral J.M. McConnell, U.S. Navy (Ret) and Edward J. Giorgio, "Building Information Security Layer by Layer." U.S. Naval Institute Proceedings, December 1998, 46.

²⁷ Ronald K. Newland, "Tactical Deception in Information Warfare: A New Paradigm for C4I." Journal of Electronic Defense, December 1998, 47.

²⁸ Vice Admiral Arthur K. Cebrowski, U.S. Navy and John J. Garstka, "Network-Centric Warfare, Its Origin and Future." U.S. Naval Institute Proceedings, January 1998, 33.

²⁹ LtGen Paul K. Van Riper, USMC, "Information Superiority." Marine Corps Gazette, June 1997, 56.

Bibliography

- Ackerman, Robert K. " Battlespace System Offers Data Anywhere, Anytime." Signal, January 1997, 26-29.
- Arquilla, John and Ronfeldt, David. Cyberwar is Coming. Santa Monica: Rand National Defense Research Institute, 1992.
- Barnett, Thomas P.M. "The Seven Deadly Sins of Network-Centric Warfare." US Naval Institute Proceedings, January 1999, 36-39.
- Brown, C. R. "The Principles of War." US Naval Institute Proceedings, June 1949, Vol. No. 75, No. 6, 621-633.
- Campen, Alan D. "Joint Vision Initiates Big Challenge To Acquisition, Integration, Culture." Signal, October 1997. <<http://www.us.net/signal/Archive/Oct97/joint-oct.html>> (23 December 1998).
- Catudal, Joseph T. The Road to Information Dominance: "System of Systems" Concept of the United States Armed Forces. Carlisle Barracks, PA: US Army War College, 06 April 1998.
- Cebrowski, Arthur K. and Garstka, John H. "Network-Centric Warfare – Its Origin and Future." US Naval Institute Proceedings, January 1998, 28-36
- Clausewitz, Carl Von. On War. Michael Howard and Peter Paret ed. Princeton: Princeton University Press, 1984.
- Cleaves, Jon S. In Search of an Enduring Military Theory: An Examination of the US Army's Principles of War. Fort Leavenworth, KS: Army Command and General Staff College, 06 June 1997.
- Clemins, Archie. "IT21: Moving to the 3rd Stage." US Naval Institute Proceedings, May 1997, 51-54.
- Delamer, Guillermo R. "The Strategic Keyboard: A Model to Relate the Principles of War." Naval War College Review, Autumn 1991, 96-107.
- Fitzgerald, James R., Christian, Raymond J. and Manke, Robert C. "Network-Centric Antisubmarine Warfare." US Naval Institute Proceedings, September 1998, 92-95.
- Glenn, Russell W. "No More Principles of War?" Parameters, Spring 1998, 48-66.
- Gourley, Robert D. "The Devil Is In the Details." US Naval Institute Proceedings, September 1997, 86-88.

- Gregory, Bill. "From Stovepipes To Grids." Armed Forces Journal International, January 1999, 18-19.
- Hammes, T. X. "War Isn't a Rational Business." US Naval Institute Proceedings. July 1998, 21-25.
- Handel, Michael I. Masters of War: Classical Strategic Thought. 2nd, Revised Edition. Portland, OR: Frank Cass, 1996.
- Hengst, P. T. Managing the Intelligent Information Grid for the Army After Next. Carlisle Barracks, PA: US Army War College, 01 April 1997.
- Jenkins, James T. "Use Technology...BUT DON'T TRUST IT!" US Naval Institute Proceedings, August 1998, 68-70.
- Johnsen, William T., Johnson II, Douglas V., Kievit, James O., Lovelace, Jr., Douglas C., and Metz, Steven. The Principles of War in the 21st Century: Strategic Considerations. Carlisle Barracks, PA: US Army War College, Strategic Studies Institute, 1 August 1995.
- Joint Warfighting Center. Concepts for Future Joint Operations: Expanding Joint Vision 2010. Fort Monroe, May 1997.
- Libicki, Martin C. The Mesh and the Net: Speculations on Armed Conflict in a Time of Free Silicon. Washington: National Defense University, Institute for National Strategic Studies, McNair Paper 28, March 1994.
- Lum, Zachary. "Hardcore Hard Kill: Seeds of a New SEAD." Journal of Electronic Defense, February 1997, 32-34.
- McConnell, J.M. and Giorgio, Edward J. "Building Information Security Layer by Layer." US Naval Institute Proceedings, December 1998, 44-47.
- Mitchell, Ross. "Naval Fire Support, Ring of Fire." US Naval Institute Proceedings, November 1997, 54-57.
- Newland, Ronald K. "Tactical Deception in Information Warfare: A New Paradigm for C4I." Journal of Electronic Defense, December 1998, 43-48.
- Owens, William A. "The American Revolution in Military Affairs." Joint Forces Quarterly, Winter 1995-96, 37-38.
- _____. "The Emerging System of Systems." US Naval Institute Proceedings, May 1995, 35-39.

Rigby, Joseph W. "The US International Digitization Strategy." International Defense Review, 11/1995, 28-32.

Tiede, Herbert R. "Principles of War." Marine Corps Gazette, April 1995, 54-56.

U.S Atlantic Command. JWID98 Post Demonstration Report. Norfolk, VA: 1998.
Executive Summary.

U.S. Joint Chiefs of Staff. Doctrine for Joint Operations (Joint Pub 3-0) Washington, D.C.: 1 February 1995.

_____. Joint Doctrine for Command and Control Warfare (C2W) (Joint Pub 3-13.1) Washington, D.C.: 7 February 1996.

_____. Joint Vision 2010 Washington, D.C.: 1996.

_____. "Observations on the Emergence of Network-Centric Warfare." Network-Centric Warfare Information Paper. 16 December 1997.
<<http://www.dtic.mil/jcs/j6/education/warfare.html>> (6 January 1999).

Van Riper, Paul K. "Information Superiority." Marine Corps Gazette, June 1997, 54-62.

Vincent, Gary A. "New Approach to Command and Control: The Cybernetic Design." Airpower Journal, Summer 1993, 24-38.

Walsh, Edward J. "Exercise Demonstrates Benefits of Military's Network-Centric Warfare." Signal, November 1997, 16-21.

West, Jr., F.J. "Ring of Fire or Ring of Smoke?" US Naval Institute Proceedings, November 1998, 38-41.

West, Leslie. "Exploiting the Information Revolution: Network-Centric Warfare Realizes Its Promise." Sea Power, March 1998, 38-40.